



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

08/994,878 12/19/97 EPSTEIN M PHA-23.313

LM02/0316

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

EXAMINER

SONG, H

ART UNIT

PAPER NUMBER

2766

DATE MAILED:

03/16/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.
08/994,878

Applicant(s)
Epstein

Examiner
Ho S. Song

Group Art Unit
2766



☒ Responsive to communication(s) filed on Jan 7, 2000

☐ This action is **FINAL**.

☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) 1-20 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 1-20 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been
☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Art Unit: 2766

DETAILED ACTION

1. Claims 1-20 are pending. The previous grounds of rejection based on the Dolan and Krajewski patents are withdrawn in view of Applicant's arguments in the Amendment filed Jan. 07, 2000. However, newly discovered prior art has necessitated new grounds of rejection. The new grounds of rejection are presented below. The delay in citation of the newly discovered prior art is regretted.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 1-4 are rejected under 35 U.S.C. 102(e) as being anticipated by Aziz (US 5,732,137).

In claim 1, Aziz discloses receiving via the network a user's ID and reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted encrypted using a key determined from identifying information of the user in (col.2, lines 26-46, col.1, lines 40-51). Sending via the network the encrypted private key , where the

Art Unit: 2766

encrypted private key can be received and decrypted at the location of the user using the user's identifying information is disclosed by Aziz in (col.6, lines 35-43).

Claim 5 differs from claim 1 in that private key is destroyed at the location of the user. Aziz discloses this feature in (col.7, lines 10-15).

In claim 6, Aziz discloses entering a passphrase entered by the user at the user equipment in (col.2, lines 29-32).

In claims 11,15, Aziz discloses storage storing respective IDs and encrypted keys for the respective users determined from user identifying information in (col.2, lines 29-46). Reading an encrypted key from the storage with an ID corresponding to a particular user and transmitting the encrypted key to the particular user is disclosed by Aziz in (col.6,19-43).

In claim 12, see claim rejection 6.

In claim 16, see claim rejection 1 and 11.

In claim 13, Aziz teaches public key cryptography in (col.1, lines 44-48).

In claim 19, see claim rejection 1 and 6.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
5. Claims 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of Schneier.

Art Unit: 2766

In claims 7-10, Aziz discloses all the claim limitations above. However, Aziz does not disclose a computing a hash document and encrypting the hash using the user's private key. Schneier discloses this feature in (page 38, section in Signing the documents with public key cryptography and One Way Hash Functions, page 39, section in Algorithms and terminology). It would have been obvious to a person of ordinary skill in the art modify the invention of Aziz to include hash function in order to enhance and secure data security and message authentication. One of ordinary skill in the art would be motivated to use hash function because integrity mechanism implicitly provide data origin authentication and vice versa.

In claims 17-18 see claims rejection 7-10 above.

In claim 20, see claims rejection 1 and 6.

Conclusion

6. Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 7:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceeding should be directed to the group receptionist, whose telephone number is (703)305-3800.

Ho Song


GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700